AMENDMENTS TO THE DRAWINGS

Figs. 3 and 4 stand objected to for minor informalities. The attached drawing sheets include amendments to Figs. 3 and 4 to correct the minor informalities. The drawing sheets attached herewith replace the original sheets comprising Figs. 3 and 4.

Attachments: Replacement Sheet for Fig. 3
Replacement Sheet for Fig. 4

REMARKS

Claims 1, 4-19, 26-27, and 34-44 are currently pending in the subject application and are presently under consideration. Claims 24 and 26-27 have previously been withdrawn. Claims 1, 4, 5, 7, 12, 16, and 18 have been amended; claims 20-23 and 28-33 have been canceled; and claims 34-44 are new as shown on pp. 2-7 of the Reply. Replacement drawings have been attached herewith as indicated on p. 8 of the Reply. Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1 and 4-19 Under 35 U.S.C §112

Claims 1 and 4-19 stand rejected under 35 U.S.C. §112, first paragraph, for failing to comply with the written description requirement. This rejection has become moot, and the withdrawal of this rejection is respectfully requested in view of the herein amendment to claim 1, upon which claims 4-19 depend.

II. Rejection of Claims 1 and 4-19 Under 35 U.S.C §112

Claims 1 and 4-19 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. This rejection has become moot in view of the amendment to claim 1, upon which claims 4-19 depend, and accordingly it is respectfully requested that this rejection be withdrawn.

IV. Rejection of Claims 1, 4-6, and 9-19 Under 35 U.S.C. §103(a)

Claims 1, 4-6, and 9-19 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Rammler (US 2003/0105535) (hereinafter "Rammler") in view of Salowey (US 7,370,350) (hereinafter "Salowey"). The withdrawal of this rejection is respectfully requested for at least the following reasons. Rammler and Salowey, taken alone or taken in combination, fail to teach or suggest each and every aspect of the subject claims.

Applicants' subject application relates to implementing security within industrial control systems. In particular, a security component is employed that initially grants access for direct communication within the industrial automation device and regulates the continuing direct access to the industrial automation device by monitoring the direct communication. If a security

issue arises or is detected during the monitoring, the security component alters or discontinues direct communication access. To this end, independent claim 1 recites in part: *an access component that defines a security attribute associated with the industrial automation device, the security attribute including a location attribute and a time attribute, wherein the time attribute defines direct communication access to the industrial automation device for a predetermined amount of time;* ***a security component that regulates*** *initial and* ***continuing direct communication access to the industrial automation device based upon the security attribute, wherein the security component monitors continuing direct communication and alters or discontinues direct communication access when a security issue arises or is detected****.* Rammler and Salowey, alone or in combination, fail to teach or suggest such aspects.

Rammler generally relates to implementing a unit controller with a palm type computer-based a human machine interface (hereinafter "HMI"). *See* Rammler Abstract. The Rammler controller includes two primary elements, the unit controller module and the palm type HMI. *See* Rammler Abstract. Rammler discusses that the unit controller can be preconfigured by the factory with standard function blocks, and that these function blocks can be changed in the field through required user password/key from authorized personnel. *See* Rammler ¶ [0060]. Rammler further discusses that changes to the configuration of the control unit can take place at any time, including on-line control editing. *See e.g.* Rammler ¶¶ [0229]-[0232]. Rammler discusses that high security can be provided by requiring users to enter access levels and passwords when performing these configuration changes. *See* Rammler ¶ [0230]. Thus, the unit controller configuration of Rammler permits full on-line control strategy editing by an authorized user, *e.g.* add, delete function, make changes to the control strategies and interlink/strategies and loops at any time. *See* Rammler ¶ [0232]. Additionally, Rammler discusses implementing the HMI with Internet functionality by building a Web server for the HMI. *See* Rammler ¶ [0195]. Several clients (*e.g.* terminals) can then access the displays of the HMI through the Web server implementation. *See* Rammler ¶ [0195]. Rammler discusses that security provisions are incorporated to limit access to the unit controller displays and data, and these security provisions are based on either a user name and password or IP address. To this end, Rammler fails to teach or suggest the aforementioned aspects of the subject claims, and Salowey fails to cure such deficiencies.

Salowey generally relates to re-authenticating computing devices over a network using short term re-authentication data. *See* Salowey col. 1 lines 10-12. In particular, Salowey discusses techniques for re-authenticating mobile devices. *See* Salowey col. 1 lines 32-36. Some examples of when wireless device may need re-authentication are when the mobile device is powered-up or rebooted, when a user logs off the device, when the mobile device is moved to a new access point, or when the mobile device moves in and out of range of an access point. *See* Salowey col. 1 lines 51-60. Salowey accomplishes this short term or temporary re-authentication avoiding the standard authentication methods such as that of EAP-SIM in a GSM network (transmitting numerous round-trip messages) by first authenticating the mobile device to a second computing device in the network with a first authentication mechanism (*e.g.* EAP-SIM or 802.1x). *See* Salowey col. 2 lines 13-18. During the first authentication, short term re-authentication data/credential is generated and issued to the mobile computing device. *See* Salowey col. 2 lines 18-20. When the need for re-authentication arises such as during a reboot of the system or moving out of range of an access point as discussed above, the mobile device sends a request to re-authenticate to the second computing device. *See* Salowey col. 2 lines 20-22. The mobile computing device then re-authenticates to the second computing device in a challenge-response fashion by presenting the short-term re-authentication credential generated during the previous authentication session, thus resulting in a shorter authentication mechanism with fewer messages exchanged. *See* Salowey col. 2 lines 22-28. It is respectfully submitted that the generation of a short-term re-authentication credential during a previous authentication session fails to cure the deficiencies of Rammler.

As discussed above, applicants' subject application relates to the regulation of direct communication access through a security component for an industrial automation device. In particular, claim 1 recites: *a security component that regulates initial and continuing direct communication access to the industrial automation device based upon the security attribute.* Therefore, in addition to regulating the initial direct communication access with the industrial automation device, the security component… regulates *continuing direct communication access to the industrial automation device.* Rammler merely describes regulating initial access to either the modification to the configuration file or by regulating the initial access to the Web-based HMI display. Rammler merely discusses that authorized personnel can edit the configuration files (including the on-line editing which is the editing while the controller is in operation) if the

authorized personnel enters the appropriate access level and password associated with such access level upon attempting to edit the configuration. Rammler does not discuss regulating access beyond or regulating the continuous direct communication access beyond the user name and password login (*e.g.* initial access). Similarly, Rammler discusses security measures with respect to accessing the Web-based HMI, but Rammler fails to teach or suggest that such access extends beyond the initial login to the HMI display through the Web-server with the username/password and/or correct IP address. Therefore, Rammler does not teach or suggest any form of regulation of continuous direct communication access to the automation device.

Salowey fails to cure the deficiency of Rammler, because as discussed above, Salowey merely relates to creating a short-cut for re-authentication by generating a temporary authentication credential during a previous authentication session. Thus, during an instance where the re-authentication is needed, such as when the authenticated device reboots, then Salowey's technique allows for a re-authentication with a simple challenge-response mechanism using the temporary credential known to both devices because it was generated between the devices during the previous authentication. Such short term re-authentication fails to teach or suggest a security component that regulates both *initial and continuing direct communication access* to the industrial automation device based upon the security attribute. Therefore, Rammler and Salowey, alone or in combination, fail to teach or suggest all aspects of claim 1, and the rejection of claim 1 should be withdrawn.

Moreover, claim 1 recites: *wherein the security component monitors continuing direct communication and alters or discontinues direct communication access when a security issue arises or is detected*. The cited art of record fails to teach or suggest such aspects. As discussed above, Rammler is only concerned with username and password/key security with respect to allowing access to configure the unit controller module, or similarly, Rammler restricts access to the Web-based HMI display to correct user name credentials through a username, password, or IP address. Thus, Rammler limits its discussion of security measures to permitting *entry* or *initial* access to the configuration or HMI through username, password, and/or IP address. As such, Rammler does not does not teach or suggest monitoring continuous direct communications and changing or preventing direct access based on issues detected by this monitoring, particularly, the security component monitors continuing direct communication and alters or discontinues direct communication access when a security issue arises or is detected, as recited

in claim 1. Salowey fails to make up for the deficiencies of Rammler because Salowey only relates to re-authenticating, or giving access reactively when the initial authorization is lost because the device has dropped the authorization (by rebooting the device, or moving out of range of an access point in a wireless network). The *reactive* re-authorization of Salowey is distinguishable the claimed subject matter because Salowey does not teach or suggest the monitor of direct communications and *alters or discontinues direct communication access when a security issue arises or is detected*. Thus, the re-authorization with a temporary credential is not altering or discontinuing direct communication access *when* a security issue arises or is detected.

Additionally, although Salowey discusses setting an expiry date/time policy within its temporary re-authentication credential (*see* Salowey col. 7 lines 33-48), such expiry policy is pre-set and expires the re-authentication based on the setting, in contrast to expiring the re-authentication (and consequently direct communication access) based on security issues that arise or are detected. To this end, it is respectfully submitted that Salowey fails to cure the deficiencies of Rammler with respect to the altering or discontinuing direct communication access of claim 1. Therefore, Rammler and Salowey, alone or in combination, fail to teach or suggest each and every aspect of claim 1, and claims 4-6 and 9-19 that depend from claim 1. In view of the foregoing, it is respectfully requested that this rejection be removed.

Claim 12 is patentable for at least the same reasons as discussed above. Moreover, claim 12 recites: ***the security parameters and policies further comprising at least one of integrity algorithms or privacy algorithms***. Claim 12 depends upon claim 11 which recites: *[t]he system of claim 1, further comprising security parameters and policies that are developed for physical and electronic security for various component types*. Each of Rammler and Salowey are silent with respect to such aspects, particularly because Rammler merely relates the security access based on the password/key or IP address of an authorized user and Salowey merely relates to the temporary re-authentication credential. To this end, Rammler and Salowey, taken together or taken separately, fail to teach or suggest all aspects of claim 12. In view of the foregoing, it is respectfully requested that the rejection of claim 12 be withdrawn.

In addition, claim 18 is patentable for at least the same reasons as discussed above. Furthermore, claim 18 recites: ***a security switch to control network access to a device or network***. Rammler and Salowey, alone or in combination, fail to teach or suggest such aspects.

As discussed above, the security implemented in Rammler is based on initial access through user password/key (including distinctions with different access levels) and IP addresses. Such security access in Rammler is not a security *switch* to control network access to a device or network. Salowey fails to cure the deficiencies with respect Rammler for claim 18 because Salowey fails to teach or suggest the aforementioned aspects with respect to the Salowey temporarily re-authentication credential. To this end, Rammler and Salowey, taken alone or taken together, fail to teach or suggest all aspects of claim 18. It is thus respectfully requested that the rejection of claim 18 be removed.

Based on the foregoing discussion, it is respectfully submitted that Rammler and Salowey, alone or in combination, fail to teach or suggest each and every aspect of claim 1, and claims 4-6 and 9-19 that depend from claim 1. Accordingly, it is respectfully requested that this rejection be withdrawn.

Similar to, though not the same as, the distinguishing features discussed with respect to at least claim 1 above, new claims 34 and 42 also patentably define over Rammler and Salowey, considered alone or together. As discussed above, Rammler relates to the modification of the controller configuration through password/key authentication at different levels of access or allowing access to the Web-based HMI display through a username and password or IP address. Salowey merely relates to generating and using a temporary re-authentication credential during a previous authenticated session. However, merely discussing allowing the initial access to the configuration files or allowing initial access to the Web-based HMI as is done in Rammler or discussing the implementation of a temporary re-authentication credential as in Salowey cannot be said to teach or suggest ***monitor the direct communication access; and modify or terminate the direct communication access when a security event is detected during the monitor of the direct communication access*** as recited in new claim 34. Furthermore, for similar reasons, Rammler and Salowey cannot be said to teach or suggest ***monitoring the direct communication access by the entity; and modifying the direct communication access when a security event is detected during the monitoring of the direct communication access*** as recited in new claim 42. Claims 35-41 and 43-44 depend from claims 34 and 42, respectively, and are believed allowable at least for the same reasons. In addition, claim 43, which depends upon claim 42, recites: ***wherein the modifying includes terminating the direct communication access when a security event is detected during the monitoring of the direct communication access***. As discussed

above, Rammler and Salowey each relate to allowing initial access or to authentication, which is readily distinguishable from *terminating* the direct communication access. To this end, claim 43 is believed to be allowable over the cited art of record.

V. Rejection of Claim 7 Under 35 U.S.C. §103(a)

Claim 7 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Rammler in view of Salowey as applied to claim 5, and further in view of Hammer, *et al.* (US 2008/0016569) (hereinafter "Hammer"). The withdrawal of this rejection is respectfully requested for at least the following reasons. Claim 7 depends upon claim 5. Claim 5 depends from claim 1 and accordingly is patentable for at least the same reasons as discussed above with respect to claim 1. Hammer generally relates to a security management system that logs or keeps records of security incidents and the responses taken by security personnel in response to these incidents within a computer system. *See* Hammer ¶¶ [0001], [0012], [0013]. Thus, Hammer fails to cure the deficiencies of Rammler and Salowey as discussed above with respect to claim 1. Accordingly, Rammler, Salowey, and Hammer fail to teach or suggest all aspects the claims that depend from claim 1, including claim 7, and it is respectfully requested that the rejection of claim 7 be withdrawn.

VI. Rejection of Claim 8 Under 35 U.S.C. §103(a)

Claim 8 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Rammler as modified by Salowey and Hammer as applied to claim 7, and further in view of Schleiss, *et al.* (US 2003/0014500) (hereinafter "Schleiss"). The withdrawal of the rejection of claim 8 is respectfully requested for at least the following reasons. Claim 8 is patentable for at least the same reasons as discussed above with respect to claim 7, upon which claim 8 depends.

Moreover, Schleiss generally relates to a transactional data communications system that communicates information within an enterprise having a process control system and a plurality of information technology systems. *See* Schleiss Abstract. The information technology systems of Schliess are communicatively coupled to the process control system via a web services interface and a transactional information server. *See* Schleiss Abstract. However, Schleiss only discusses implementing security similar to that of Rammler by implementing web services that perform security checks based on initial user authentication and verification. *See* Schleiss ¶

[0053]. To this end, Schleiss fails to cure the aforementioned deficiencies of claim 1 as discussed above. Accordingly, Rammler, Salowey, Hammer, and Schleiss, alone or in combination, fail to teach or suggest all aspects of claim 7 and claim 8 that depends therefrom. Thus, it is respectfully requested that the rejection of claim 8 be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [ALBRP303USA].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

TUROCY & WATSON, LLP

/Adam P. Slepecky/

Adam P. Slepecky
Reg. No. 61,170

TUROCY & WATSON, LLP
57TH Floor, Key Tower
127 Public Square
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731